VZCZCXRO1052
RR RUEHAG RUEHDF RUEHIK RUEHLZ RUEHPOD RUEHROV
DE RUEHC #7237/01 1931858
ZNR UUUUU ZZH
R 121844Z JUL 07
FM SECSTATE WASHDC
TO EU MEMBER STATES COLLECTIVE
INFO EU INTEREST COLLECTIVE

UNCLAS SECTION 01 OF 06 STATE 097237

SIPDIS

SIPDIS

E.O. 12958: N/A
TAGS: PTER PREL EAIR PINR KTIA KHLS CVIS EUN
SUBJECT: U.S., EUROPEAN UNION CONCLUDE NEGOTIATIONS ON A PASSENGER NAME RECORD (PNR) AGREEMENT

¶1. (U) Summary: On Thursday June 28, 2007, the United States and the European Union (EU) concluded negotiations on a Passenger Name Record (PNR) Agreement. This new agreement will replace an interim agreement concluded in 2006 between the United States and the EU that was set to expire on July 31, 2007. The agreement ensures that PNR data may be used by the USG to combat terrorism and serious transnational crime while satisfying the European Union,s concerns about the protection of the privacy of European citizens. The new agreement also provides air carriers legal certainty that they will not be in potential violation of European privacy law if they comply with U.S. law concerning PNR. The signing of this new PNR agreement will ensure that the Department of Homeland Security (DHS) can continue to effectively use PNR data to protect border security and to conduct counterterrorism operations, including preventing dangerous people from boarding planes and entering the United States.

¶2. (U) Talking points (paragraph 17) and a list of Frequently Asked Questions (FAQ) (paragraph 18) cleared for use by all USG officials are included at the end of this cable. However, detailed conversations about the content of the agreement should be avoided until after the text has been signed and released.

- History of the Passenger Name Record -

¶3. (U) Customs and Border Protection (CBP), an agency within DHS, began using electronic PNR data from air carriers on a voluntary basis in 1996. According to the Aviation and Transportation Security Act of 2001, as implemented at title 19, Code of Federal Regulations, section 122.49d, air carriers operating passenger flights to or from the United States must provide CBP with access to PNR data that is in its automated reservation/departure control system. This data is stored in and processed by DHS through the Automated Targeting System (ATS).

¶4. (U) PNR data is a limited set of information collected by travel agents and airlines about air passengers. It is collected by airlines and travel agents as part of their normal business processes per their individual business models. PNR data may include information such as: name, contact information, payment method, and information about a passenger,s baggage.

¶5. (U) PNR data provides the United States with the means to make connections between known threats and associates; it allows us to identify patterns of activity that can help us identify persons of concern. PNR is different from the Advance Passenger Information (API), which is verified information that is used to check names against terrorist watchlists and other law enforcement databases. In combination with APIS, PNR is especially important for screening passengers coming from visa-waiver countries, because these passengers have not been required to submit information to the United States prior to the flight to obtain a visa.

- European Reaction -

¶6. (U) In 2002, the European Union raised concerns that the requirement to submit PNR information conflicted with its Directive 95/46/EC (&the European Data Protection Directive8). The European Data Protection Directive places burdens on data controllers operating under community law that limit their ability to share personal data with public or private entities in non-EU countries without a demonstration that the receiving entity has adequate data protection standards. There was a perceived risk that, absent such agreement, any carrier complying with U.S. law would be at risk of fines or other penalties under the Data Protection Directive or implementing Member State law.

¶7. (U) The 2004 PNR agreement between the United States and the European Community (EC) sought to remedy these concerns, by allowing airlines to legally provide the United States access to PNR data while giving the EC detailed assurances on how CBP would collect, process, handle, protect, share and ensure oversight of PNR data (such assurances were referred to as the &Undertakings8).

¶8. (U) Subsequent to the signing of this 2004 agreement, the European Parliament brought a case before the European Court of Justice (ECJ) against the European Commission and Council of the European Union for signing the agreement. The European Parliament challenged both the authority of the Commission

and Council to enter into the agreement without Parliament,s assent, as well as the merits) whether the Undertakings issued by CBP were adequate to meet EU data protection requirements.

¶9. (U) In 2006, the ECJ ruled on the Council,s authority to enter into an agreement on PNR with DHS. The ECJ did not rule whether the US-EU agreement infringed fundamental rights with regard to data protection, nor did it rule against the availability of PNR data or comment on the actual content of the agreement; rather, the ECJ ruled that the legal basis upon which the EU entered into the agreement was inapplicable.

¶10. (U) According to the ECJ ruling, any new PNR agreements would have to be under the EU,s &third pillar,8 which includes law enforcement and public security issues and is a shared competence between the European Institutions and the EU member states. The ECJ gave the European Union until September 30, 2006 to terminate the 2004 Agreement.

- The Interim Agreement -

¶11. (U) On October 19, 2006, the United States signed an interim agreement with the European Union (EU) on PNR data, which was accompanied by a &unilateral8 letter of interpretation of U.S. obligations under the agreement. While the EU merely acknowledged the DHS letter, in fact the text was intensely negotiated with the EU as the substantive framework for the interim agreement. The interim agreement allowed greater access to PNR data by other USG agencies than under the prior agreement, and obliged air carriers to update the systems they used to transmit data to CBP. It also clarified how other provisions of the Undertakings would be implemented under the interim agreement, including sections dealing with the carrier,s transmission of PNR data, certain data elements and the vital interest clause of the agreement.

- The New Agreement -

¶12. (U) The new PNR agreement, initialed on June 28, 2007 and which is expected to be signed in July 2007 and enter into force on August 1, 2007, achieves the aims of both the United States and the European Union and will entail binding international obligations on the parties.

¶13. (U) The new agreement continues to offer a high level of privacy protection for EU PNR. The agreement enhances the public image of the collection requirement in Europe while ensuring access to all critical data. This was done in part by reducing the 34 &data elements8 to 19 &types of EU PNR collected.8 The 19 types of information to be collected by DHS have proven necessary in concluding numerous investigations and continued access to this information will be invaluable in the fight against terrorism and other serious transnational crimes, and to keep dangerous people out of the United States. According to this new agreement, DHS will hold PNR data for 7 years as an active file; after this, the data will be maintained as a &dormant8 file for 8 years with limited access. DHS will also be able to use this information across its organization, not only within CBP, to prevent terrorism and other serious crimes. Under the new PNR agreement, DHS is able to share PNR data with other USG agencies for uses consistent with the defined purposes.

¶14. (U) The new agreement also reconfirms that DHS is prepared to support a &push8 rather than a "pull" system, meaning that DHS will actively engage air carriers seeking to migrate their systems to transmit their information to DHS rather than prior arrangements, under which DHS pulled the information directly from their reservation systems. This compromise is limited to those carriers that prove able and willing to meet DHS,s technical requirements. No discretion is provided to the carriers or European authorities about how and when carriers will transmit PNR data.

¶15. (U) The signing of this new PNR agreement will ensure that DHS continues to protect border security, by keeping dangerous people from boarding planes and entering the United States. It further supports DHS,s obligation to share terrorism information with other agencies of the USG. Sharing with other agencies will be limited by the purpose definition of the agreement and the verification that receiving agencies will only be using PNR to support their case work that falls under the purpose definition. This removes significant process and technological limitations that plagued the last two agreements.

¶16. (U) DHS will follow the conclusion of this negotiation with the publication of a new System of Record Notice (SORN) and Privacy Impact Assessment (PIA) for the Automated Targeting System (the database where PNR data is stored),

which will reflect many of the protections also articulated in the agreement.

¶17. (U) Talking Points

On Thursday, June 28, 2007, Secretary Chertoff, German Interior Minister Wolfgang Sch,uble and EU Commissioner Franco Frattini initialed an international agreement between the United States and the European Union on the transfer of PNR data from air carriers serving the transatlantic market to DHS. The U.S. thanks the EU, and in particular Minister Sch,uble, for its partnership during the recent negotiations.

The new agreement ensures that all passengers traveling to the United States will benefit from a higher degree of protection against terrorist and serious transnational criminal threats while ensuring a high level of protection for their personal information. It also provides legal certainty for air carriers) ensuring that their compliance with the DHS PNR regulation does not result in enforcement activities by European data protection or other authorities.

PNR data is a proven tool for combating terrorism and serious transnational crime. It has been used in the U.S. to identify terrorist cells, dismantle human trafficking rings and arrest drug smugglers, among other successes.

The new agreement ensures that DHS can comply with its obligation under the Intelligence Reform and Terrorism Prevention Act to share terrorism information with other USG agencies, which grew out of recommendations made by the 9/11 Commission.

It ensures that PNR data is not used or shared for purposes other than which it is collected. PNR is primarily collected to combat terrorism, serious transnational crime and to protect the vital interests of the individual.

DHS and the EU have agreed to revise the list of data that may be collected while ensuring that flexibility is retained to ensure sufficient data is collected to meet current and future threats.

Under DHS policy, as detailed in the agreement, EU citizens (and any other citizen) will have many of the same administrative protections as U.S. Citizens, including the ability to obtain information held about them and to seek the correction of incorrect data.

¶18. (U) Anticipated Questions. The following section seeks to give answers to some expected questions embassy personnel might receive from government personnel and the public:

Q1. What is the difference between the interim PNR agreement that expires on July 31, 2007 and the new agreement?

A1. The new agreement improves on the previous agreement in several ways. The new agreement ensures improved privacy protection for EU citizens. In the new agreement DHS reaffirms its long standing commitment to migrate to a &push8 system for receiving PNR and establishes a deadline by which we expect carriers to make the information technology investments to affect this change. It establishes a commitment for the US and EU to work to improve notice to travelers. The data retention period is extended based on lessons learned from recent terrorism investigations reviewed by the negotiators. It reforms the description of the information that DHS collects to allow for the collection of 19 classes of data. In DHS,s experience, information falling into each of these categories has proven vital in interdicting threats and developing cases. Finally, the agreement is more balanced by establishing new reciprocal expectations and ensuring that future reviews will consider security requirements as much as data protection interests. Otherwise, the new agreement has the same purposes as the last two agreements and retains many operational requirements incorporated into the 2006 interim agreement. In particular, DHS,s ability to share PNR with other USG agencies with a counter-terrorism/law enforcement focus continues to be facilitated while DHS reaffirmed its commitment to consider such requests carefully and consistent with the purposes for which PNR is collected.

Q2. How do U.S. laws protect sensitive data?

A2. The U.S. has an extensive legal and oversight system for protecting privacy that is at least as strong as the European approach. The primary U.S. laws defining how federal agencies protect individual privacy are the Privacy Act of 1974, the Freedom of Information Act, and the E-government Act of 2002. While the rights detailed in the Privacy Act are

limited to U.S. citizens and lawful permanent residents, earlier this year, DHS administratively extended many of these protections to non-U.S. persons. Both U.S. and European privacy law are based on the Fair Information Practices and include regimes for preventing mission creep, obtaining access to and correction of data and ensuring effective oversight.

Q3. Will the U.S. privacy protections apply to the data of non-U.S. citizens collected under the PNR agreement?

A3. DHS has decided to give administrative Privacy Act protection to all PNR data contained in the Automated Targeting System, regardless of the nationality or country of residence of the person to whom the data belongs. Part of this protection includes redress, and all individuals for whom data has been collected under the PNR agreement can seek information about or correction of their PNR data. Under the Freedom of Information Act (FOIA), any person can request access to their personally identifiable information in the PNR, except in special cases when there is an applicable exception in the FOIA regulations. Travelers can seek to have their information corrected through DHS,s Traveler Redress Inquiry Program (TRIP). Directions for using both of these mechanisms are available on the DHS website.

Q4. Why does DHS need to access sensitive data, even in exceptional cases?

A4. At times law enforcement tips or intelligence may only provide limited clues by which a suspect may be identified. These clues can be limited to physical or other characteristics that may only be identifiable through sensitive data. In these extremely rare cases, the individual,s expectation of privacy is superseded by the public,s interest in preventing serious harm to other individuals. For example, if a tip revealed that a man wearing a cast and traveling on a certain date planned to blow up a plane or was smuggling young children into sexual slavery, DHS should be able to review sensitive data to identify travelers who have requested special accommodations due to a cast or leg injury. DHS does not normally use or even view sensitive data and it is deleted promptly in most cases.

Q5. Why does DHS need to share PNR data with other USG agencies? Doesn,t this contravene European privacy standards?

A5. One of the primary lessons learned by both Europe and the United States is the need for law enforcement and homeland security agencies to work more closely together and more effectively share information. Different agencies and officers can apply unique expertise and analytical tools to data to maximize the value its collection provides to the traveling public. In fact, U.S. law now requires all federal agencies that hold terrorism information to make that information available to other USG agencies. For example, after 9/11 a private firm was able to identify connections between all 19 hijackers based on their PNR) a capability the USG lacked at the time. This concept is as widely recognized in Europe as it is in the United States as evidenced by recent decisions in the EU on the Pruem Convention and law enforcement access to the Visa Information System.

Q6. How can we be sure that the United States will not transfer personal data on EU citizens to third countries that will not protect the data? Or on to those who will use the data for purposes other than intended?

A6. The United States will only transfer data to a third country after considering the recipient,s intended use of the data and its ability to protect the information. Data protection standards in this third country must instill confidence and be consistent with the national interests of the United States in order for the United States to transmit the data. These are the same standards that the EU has agreed to and has deemed to offer an adequate level of data protection.

Q7. Why was the retention period expanded from 3.5 years to 7

plus 8?

A7. The interim agreement permitted retention for some data for as long as 11.5 years but required other data to be deleted after 3.5 years. U.S. and EU negotiators recognized

that the previous retention period was insufficient to investigate terrorist plots and other activities which may take many years to come to fruition. The parties looked at a variety of specific examples and settled on the following retention period: DHS will hold PNR data in an active database for seven years. After this, the data will become dormant, and will be kept for eight years. During these eight years, the information can be accessed only in response to an identifiable threat or risk, and even then it can only be accessed with the authorization of a senior official at DHS designated by the Secretary of Homeland Security.

Q8. Will the PNR data be used for preventing or investigating pandemics or to capture perpetrators of minor crimes or anything other than terrorism and serious crimes?

A8. PNR may be used under the agreement to prevent or respond to pandemics and other public health events. The original PNR agreement and the recently superseded interim agreement both recognized this necessity. The importance of this provision was further made clear by the recent case of a U.S. citizen with drug-resistant tuberculosis who traveled to Europe potentially exposing many airline passengers to the disease. In this case, DHS provided PNR data to the Center for Disease Control (CDC) to support their contact tracing efforts. PNR can be a useful tool for contact tracing in such instances. It protects the vital interests of the data subject and others by helping to ensure exposed passengers receive prompt medical attention.

Q9. How will the new agreement impact the airlines and the summer travel season?

A9. The new agreement will make the summer travel season easier and safer. In general, the new agreement continues to ensure legal certainty that air carriers complying with the DHS PNR regulation will not be penalized under European law. This, plus the continued security benefit of PNR screening, should instill further confidence in the reliability and security of transatlantic air travel. Those air carriers that have not yet transitioned to a &push8 system should plan to do so before the end of 2007 and DHS is prepared to work with individual carriers to help them meet DHS,s technical requirements.

Q10. Hasn,t the technology to support a &push8 system been available for some time? If so, why can,t a date be established for this transition?

A10. Yes. The technology that would enable air carriers to transfer data to DHS instead of having DHS collect that information directly from their reservations system is available and 13 air carriers are currently using it. However, many air carriers have proven unable or unwilling to make the information technology investments to meet DHS,s technical requirements for the secure and effective operation of such a system. By establishing a deadline of January 1, 2008, DHS hopes those European carriers that have been slow to make this migration will redouble their efforts.

Q11. Can the U.S. decide at any time to revoke the protections for the personal data of non-U.S. citizens that the PNR agreement promises?

A11. If the European Union finds that the United States

breaches the PNR agreement initialed on June 28, 2007, including with regard to the application of the U.S. privacy laws named in the agreement to non-U.S. citizens, then the EU may terminate the agreement. In return, if the United States finds that the EU has breached the agreement, then it may likewise terminate the agreement.

Q12. Will the &Undertakings8 adopted by DHS pursuant to the 2004 agreement remain in force?

A12. No. The Undertakings are superseded by Secretary Chertoff,s assurances articulated in his letter to the EU.

Q13. Would Advance Passenger Information (API) data be sufficient to identify travellers who are suspected of terrorism or other transnational crime?

A13. No. API data is sufficient for doing a basic law enforcement check and is the primary data through which the USG vets travellers against our watchlists. PNR data, however, supports a number of screening and investigatory

capabilities beyond API. First, PNR is an extremely valuable tool for identifying the associates of watchlisted travellers, some of which may be previously unknown to law enforcement. In addition, PNR allows us to identify travellers adopting known or suspected travel patterns of criminals and terrorists without engaging in racial, ethnic or religious profiling.

Q14. Will DHS use PNR data to conduct racial profiling? Will it target specific religious or racial groups?

A14. No. DHS does not conduct racial profiling and it does not target passengers on the basis of racial, religious, or sexual orientation information that could be inferred from PNR data. Rather, PNR data is subjected to what is called &pattern analysis,8 meaning that pieces of information like credit cards and phone numbers may reveal connections to known terrorists and other criminals, or that suspicious baggage activity or other information is consistent with that of known terrorists and criminals.

Q15. How will the EU be able to review DHS, performance and make sure that it is keeping data protected as promised?

A15. The Agreement provides for a periodic review of its implementation, including any instances in which sensitive data was accessed. In the review, the EU will be represented by the Commissioner for Justice, Freedom and Security, and DHS will be represented by the Secretary of Homeland Security, or by such mutually acceptable official as each may agree to designate.

¶19. (U) Should posts have any questions, need further guidance, or wish to share host country reactions or comments on the agreement, please feel free to contact DHS, Office of International Affairs, Michael Scardaville, at (202) 282-8321, and Department of State, Office of European Union and Regional Affairs, Alessandro Nardi, at (202) 647-3843.
RICE